EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	40	identifier protection	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:01
L2	117	((device name) or (serial number) or (device identifier) or (device adj (ID))) near7 (compar$4 or match$4) near8 (decrypt$4 or unscrambl$4 or decipher$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:12
L3	0	((device name) or (serial number) or (device identifier) or (device ID)) near7 (compar$4 or match$4) near8 (decrypt$4 or unscrambl$4 or decipher$4) same (storage near protect$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:05
L4	2	((device name) or (serial number) or (device identifier) or (device ID)) near7 (compar$4 or match$4) near8 (decrypt$4 or unscrambl$4 or decipher$4) and (storage near protect$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:05
L5	11	((device name) or (serial number) or (device identifier) or (device ID)) near7 (compar$4 or match$4) near8 (decrypt$4 or unscrambl$4 or decipher$4) and (storage near4 protect$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:07
L6	55	((device name) or (serial number) or (device identifier) or (device adj (ID))) near7 (compar$4 or match$4) near8 (decrypt$4 or unscrambl$4 or decipher$4) same stored	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:23
L7	1	(original version).clm. and storage. clm. and first.clm. and second.clm. and encrypted.clm. and information. clm. and decrypt$4.clm. and key. clm. and compar$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/28 15:25
S1	1753	(compar$4 or match$4) same stored same (data or text or document or identification or identifier or "ID" or content) near5 (encrypted or ciphered or scrambled)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/06/14 09:00

EAST Search History

S2	1753	(compar$4 or match$4) same stored same ((data or text or document or identification or identifier or "ID" or content) near5 (encrypted or ciphered or scrambled))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/12 16:01
S3	138	(compar$4 or match$4) near5 stored near5 ((data or text or document or identification or identifier or "ID" or content) near5 (encrypted or ciphered or scrambled))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 08:06
S4	2	"5365587".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 09:31
S5	620	((decrypt$3 or decipher$) near5 (compar$4 or match$4)) same ((storage or verif$4 or authenticat$4) near5 (data or text or content or identification or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 09:34
S6	620	((decrypt$3 or decipher$) near5 (compar$4 or match$4)) same ((storage or verif$4 or authenticat$4) near5 (data or text or content or identification or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 09:35
S7	103	((decrypt$3 or decipher$) near5 (compar$4 or match$4)) same ((storage or verif$4 or authenticat$4) near5 (data or text or content or identification or identifier)) same (alter$3 or chang$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 09:52
S8	1216	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 12:11
S9	39	stored data protection	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:01
S10	1	compar$3 near9 request near9 (data$1type or data$1block or data$1structure or identifier) near9 (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:05

EAST Search History

S11	4	compar$3 near9 (user) near9 (data$1type or data$1block or data$1structure or identifier) near9 (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:06
S12	44	compar$3 near9 (payload or data$1type or data$1block or data$1structure or identifier) near9 (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:12
S13	1611	compar$3 near10 (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:12
S14	1292	match$3 near10 (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:13
S15	101	match$3 near (transmit$4 or send$3 or provid$3) near4 (content or music or e$6data)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:13
S16	101	match$3 near (transmit$4 or send$3 or provid$3) near4 (content or music)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 10:13
S17	0	713/193.ccls. and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 12:12
S18	12	713/193.ccls. and S13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/13 12:12
S19	16	(compar$4 or match$4) same (original or clear) same ((re$1 (encrypted or $2ciphered or scrambled)) or ((twice or multipl$3) near (encrypted or ciphered or enciphered or scrambled))) same stored	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/06/14 09:05

Terms used
original version and storage and first and second and encrypted and information and decrypt$4 and key and compar$4

Found 101,366 of 186,958

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next
Best 200 shown

Relevance scale

1 GPGPU: general purpose computation on graphics hardware
David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ian Buck, Cliff Woolley, Aaron Lefohn
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(63.03 MB) Additional Information: full citation, abstract, citings

The graphics processor (GPU) on today's commodity video cards has evolved into an extremely powerful and flexible processor. The latest graphics architectures provide tremendous memory bandwidth and computational horsepower, with fully programmable vertex and pixel processing units that support vector operations up to full IEEE floating point precision. High level languages have emerged for graphics hardware, making this computational power accessible. Architecturally, GPUs are highly parallel s ...

2 Improved proxy re-encryption schemes with applications to secure distributed storage
Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger
February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1
Publisher: ACM Press
Full text available: pdf(331.59 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

3 Physical privacy: Privacy management for portable recording devices
J. Alex Halderman, Brent Waters, Edward W. Felten
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**
Publisher: ACM Press
Full text available: pdf(321.69 KB) Additional Information: full citation, abstract, references, index terms

The growing popularity of inexpensive, portable recording devices, such as cellular phone cameras and compact digital audio recorders, presents a significant new threat to privacy. We propose a set of technologies that can be integrated into recording devices to provide stronger, more accurately targeted privacy protections than other legal and technical measures now under consideration. Our design is based on an informed consent principle, which it supports by the use of novel devices and pr ...

Keywords: camera phones, privacy, recording devices

4 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels
Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**
Publisher: ACM Press
Full text available: Additional Information:

pdf(6.06 MB) full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

5 File and storage systems: Preserving peer replicas by rate-limited sampled voting

Petros Maniatis, David S. H. Rosenthal, Mema Roussopoulos, Mary Baker, TJ Giuli, Yanto Muliadi

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: pdf(336.27 KB) Additional Information: full citation, abstract, references, citings, index terms

The LOCKSS project has developed and deployed in a world-wide test a peer-to-peer system for preserving access to journals and other archival information published on the Web. It consists of a large number of independent, low-cost, persistent web caches that cooperate to detect and repair damage to their content by voting in "opinion polls." Based on this experience, we present a design for and simulations of a novel protocol for voting in systems of this kind. It incorporates rate limitation an ...

Keywords: digital preservation, rate limiting, replicated storage

6 DISP: Practical, efficient, secure and fault-tolerant distributed data storage

Daniel Ellard, James Megquier

February 2005 **ACM Transactions on Storage (TOS)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: pdf(148.11 KB) Additional Information: full citation, abstract, references, index terms

DISP is a practical client-server protocol for the distributed storage of immutable data objects. Unlike most other contemporary protocols, DISP permits applications to make explicit tradeoffs between total storage space, computational overhead, and guarantees of availability, integrity, and privacy on a per-object basis. Applications specify the degree of redundancy with which each item is encoded, what level of integrity checks are computed and stored with each item, and whether items are stor ...

Keywords: Distributed data storage

7 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren

November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**

Publisher: IBM Press

Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

8 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems

Vishal Kher, Yongdae Kim

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

9 Software protection and simulation on oblivious RAMs

Oded Goldreich, Rafail Ostrovsky

May 1996 **Journal of the ACM (JACM)**, Volume 43 Issue 3

Publisher: ACM Press

Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

10 Distributed file systems: concepts and examples

Eliezer Levy, Abraham Silberschatz

December 1990 **ACM Computing Surveys (CSUR)**, Volume 22 Issue 4

Publisher: ACM Press

Full text available: pdf(5.33 MB) Additional Information: full citation, abstract, references, citings, index terms, review

The purpose of a distributed file system (DFS) is to allow users of physically distributed computers to share data and storage resources by using a common file system. A typical configuration for a DFS is a collection of workstations and mainframes connected by a local area network (LAN). A DFS is implemented as part of the operating system of each of the connected computers. This paper establishes a viewpoint that emphasizes the dispersed structure and decentralization of both data and con ...

11 Improving key predistribution with deployment knowledge in static sensor networks

Donggang Liu, Peng Ning

November 2005 **ACM Transactions on Sensor Networks (TOSN)**, Volume 1 Issue 2

Publisher: ACM Press

Full text available: pdf(639.52 KB) Additional Information: full citation, abstract, references, index terms

Pairwise key establishment is a fundamental security service for sensor networks. However, establishing pairwise keys in sensor networks is a challenging problem, particularly due to the resource constraints on sensor nodes and the threat of node compromises. This article proposes to use both *predeployment and postdeployment knowledge* to improve pairwise key predistribution in static sensor networks. By exploiting the predeployment knowledge, this article first develops two key predistrib ...

Keywords: Sensor networks, key management, key predistribution

12 The LOCKSS peer-to-peer digital preservation system

Petros Maniatis, Mema Roussopoulos, T. J. Giuli, David S. H. Rosenthal, Mary Baker

February 2005 **ACM Transactions on Computer Systems (TOCS)**, Volume 23 Issue 1

Publisher: ACM Press

Full text available: pdf(715.30 KB) Additional Information: full citation, abstract, references, index terms

The LOCKSS project has developed and deployed in a world-wide test a peer-to-peer system for preserving access to journals and other archival information published on the Web. It consists of a large number of independent, low-cost, persistent Web caches that cooperate to detect and repair damage to their content by voting in "opinion polls." Based on this experience, we present a design for and simulations of a novel protocol for voting in systems of this kind. It incorporates rate l ...

Keywords: Rate limiting, digital preservation, replicated storage

13 Decentralized storage systems: Ivy: a read/write peer-to-peer file system

Athicha Muthitacharoen, Robert Morris, Thomer M. Gil, Benjie Chen

December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI

Publisher: ACM Press

Full text available: pdf(1.65 MB) Additional Information: full citation, abstract, references

Ivy is a multi-user read/write peer-to-peer file system. Ivy has no centralized or dedicated components, and it provides useful integrity properties without requiring users to fully trust either the underlying peer-to-peer storage system or the other users of the file system.An Ivy file system consists solely of a set of logs, one log per participant. Ivy stores its logs in the DHash distributed hash table. Each participant finds data by consuiting all logs, but performs modifications by appendi ...

14

On randomization in sequential and distributed algorithms
Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms— both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

15 Digital signets: self-enforcing protection of digital information (preliminary version)
Cynthia Dwork, Jeffrey Lotspiech, Moni Naor
July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(1.24 MB) Additional Information: full citation, references, citings, index terms

16 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

17 Integrating security in a large distributed system
M. Satyanarayanan
August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3
Publisher: ACM Press
Full text available: pdf(2.90 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

18 Modeling and assessing inference exposure in encrypted databases
Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani Di Vimercati, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati
February 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 1
Publisher: ACM Press
Full text available: pdf(727.96 KB) Additional Information: full citation, abstract, references, index terms

The scope and character of today's computing environments are progressively shifting from traditional, one-on-one client-server interaction to the new cooperative paradigm. It then becomes of primary importance to provide means of protecting the secrecy of the information, while guaranteeing its availability to legitimate clients. Operating online querying services securely on open networks is very difficult; therefore many enterprises outsource their data center operations to external applicati ...

Keywords: Cryptography, database service, indexing, inference

19 Intrusion detection and modeling: Augmenting storage with an intrusion response primitive to ensure the security of critical data
Ashish Gehani, Surendar Chandra, Gershon Kedem
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(326.59 KB) Additional Information: full citation, abstract, references

Hosts connected to the Internet continue to suffer attacks with high frequency. The use of an

intrusion detector allows potential threats to be flagged. When an alarm is raised, preventive action can be taken. A primary goal of such action is to assure the security of the data stored in the system. If this operation is effected manually, the delay between the alarm and the response may be enough for an intruder to cause significant damage.The alternative proposed in this paper is to provide a re ...

20 PocketLens: Toward a personal recommender system

Bradley N. Miller, Joseph A. Konstan, John Riedl

July 2004 **ACM Transactions on Information Systems (TOIS)**, Volume 22 Issue 3

Publisher: ACM Press

Full text available: pdf(1.10 MB) Additional Information: full citation, abstract, references, index terms

Recommender systems using collaborative filtering are a popular technique for reducing information overload and finding products to purchase. One limitation of current recommenders is that they are not portable. They can only run on large computers connected to the Internet. A second limitation is that they require the user to trust the owner of the recommender with personal preference data. Personal recommenders hold the promise of delivering high quality recommendations on palmtop computers, e ...

Keywords: Collaborative Filtering, Peer-to-Peer Networking, Privacy, Recommender Systems

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next